AUTOMATIZACIÓN PARA EL CONTROL DE ACCESO UTILIZANDO DISPOSITIVOS MÓVILES Y RFID

Rafael de la Rosa Flores
Benemérita Universidad Autónoma de Puebla
rafa_elo31@hotmail.com

David E. Munoz Morales
Benemérita Universidad Autónoma de Puebla
devasc26@gmail.com

Ervic Pérez Mendoza
Benemérita Universidad Autónoma de Puebla
chivis_luis@hotmail.com

José Luis Mora Flores
Benemérita Universidad Autónoma de Puebla
chivis_luis@hotmail.com

Hilda Castillo Zacatelco
Benemérita Universidad Autónoma de Puebla
hildacz@gmail.com

Resumen

Este documento describe un proyecto que utiliza diferentes elementos tecnológicos, tanto software como hardware que permiten automatizar y controlar el acceso a un sitio. Se implementó una arquitectura de hardware con tecnología de identificación de radio frecuencias, RFID, un dispositivo Arduino y un dispositivo Ethernet shield para controlar el acceso. En el caso del software, se implementa una arquitectura de tres capas y dos niveles que interactúa con la arquitectura del hardware. Asimismo, se desarrolló una aplicación móvil que gestiona a los

usuarios que tienen acceso al sitio, que puede ser una casa u oficina, entre otros. En particular, el proceso de automatización fue desarrollado e implementado para que los estudiantes de la FCC de BUAP puedan acceder a los laboratorios.

La automatización del acceso al laboratorio permite saber a quién y en qué momento los usuarios hacen uso del laboratorio, ya que los accesos se almacenan en una base de datos y se visualizan en un dispositivo móvil.

Palabra(s) Clave: Arquitectura de SW y HW, Control de acceso, Dispositivos móviles, RFID.

Abstract

This document presents a project that uses different technological elements, both software and hardware that allow to automate and control access to a site. A hardware architecture was implemented using RFID technology, an Arduino device and an Ethernet shield device to control access. For the software case, a 3-layer, two-tier architecture is implemented and interacts with the hardware architecture. As well, a mobile application was developed that manages the users that have access to the site, which can be a house, official, among others. In particular, the process of automation was developed and implemented so that students of the FCC of BUAP can access the laboratories.

The automation of the access to the laboratory allows to know who and at what time the users make use of the laboratory, since the accesses are stored in a database and are visualized in a mobile device.

Keywords: *Access control, Mobil device, RFID, Software and hardware architecture.*

1. Introducción

El acceso a algunos sitios requiere de tener mecanismos automatizados seguros y confiables que autentiquen a las personas que acceden a los mismos. Esto permite tener bitácoras de accesos que den seguimiento a los usuarios que hacen uso de las instalaciones, ya que en caso de pérdidas o daños a los elementos dentro del sitio se tendría conocimiento de los involucrados. Motivo por

el cual, es indispensable contar con soluciones tecnológicas que permitan acreditar a los usuarios que acceden a sitios de alta seguridad.

La domótica o "*home automation*", es un conjunto de elementos tecnológicos que ayudan a automatizar una vivienda, esto incluye procesos, sistemas, dispositivos electrónicos o mecánicos que realizan la labor que normalmente hacen las personas. De manera particular, el acceso a un sitio es fundamental dentro de este contexto. Para acceder a un sitio, existen diferentes elementos tecnológicos que permiten obtener información de las personas y autenticarlas. Por ejemplo, lectores biométricos, de iris, lectores de radiofrecuencias, entre otros.

En este documento se presenta una propuesta funcional que automatiza el acceso a un sitio de alta seguridad utilizando algunos elementos tecnológicos, tales como: identificador de radio frecuencias, RFID [Phillips, 2005], placa Arduino uno, servidor de bases de datos, dispositivos móviles, entre otroscomponente de software y hardware que automatizan el acceso de las personas a un sitio. En particular se desarrolló e implementó el proceso de automatización para que los estudiantes de la FCC de la BUAP accedan a los laboratorios. La automatización del acceso al laboratorio permite conocer quiénes son y en qué momento los usuarios hacen uso del mismo, ya que se almacenan los accesos en una base de datos y se visualizan tanto en un servidor como en un dispositivo móvil.

A la fecha existen diferentes trabajos [Kovatsch, 2010], que utilizan cámaras, detectores de movimiento y dispositivos móviles para monitorear sitios de alta seguridad. Algunos utilizan el Bluetooth y teléfonos inteligentes para desarrollar un sistema de seguridad que permite bloquear o desbloquear el acceso a un sitio [Potts, 2012]. Un trabajo interesante es el reportado en [Rajadurai, 2015], éste utiliza algunos elementos tecnológicos tales como un controlador ARM con sensores IR que permiten detectar a una persona y utilizan SMS para autenticar. Existen otros trabajos, por ejemplo, en Das [2011] y Piyare [2011], utilizan elementos tecnológicos como dispositivos móviles y Bluetooth para automatizar los dispositivos electrónicos de una casa.

En la siguiente sección se explica el desarrollo y la implementación del mecanismo de automatización.

2. Metodología

Aunque la tecnología de identificación de radiofrecuencias no es nueva, en la última década ha sido ampliamente difundida y utilizada en aplicaciones cotidianas [Ugarte, 2017]. Una de las características básicas que proporciona este tipo de tecnologías es la capacidad de proveer un identificador único y que permite rastrear objetos a cierta distancia. Estas condiciones motivaron a utilizar la tecnología RFID como componente de autenticación para el desarrollo del proyecto, así como también se utiliza un dispositivo móvil para rastrear y administrar los accesos al sitio, entre algunos otros elementos.

El esquema general del mecanismo de automatización se divide en dos arquitecturas: de software y de hardware, que a continuación se explican.

Arquitectura de hardware

Los dispositivos de hardware que se consideran en este proyecto para automatizar el acceso son:

- Módulo RFID RC522
- Placa Arduino uno
- Tag ID`s
- Selenoide
- Placa Ethernet Shield
- Servidor de Almacenamiento

La arquitectura general del mecanismo de hardware que automatiza el acceso se muestra en la figura 1. De manera permanente la placa Arduino se encuentra enviando peticiones de lectura, cuando el lector de RFID recibe la instrucción de realizar una lectura, éste envía una señal al ambiente de búsqueda de etiquetas de RFID, si encuentra alguna, obtendrá su número de identificación y lo enviará de vuelta a la computadora. Después el módulo de control de acceso procesará este identificador y decidirá si el usuario tiene permitido el acceso. Si esto es verdadero, entonces se envía una señal a la tarjeta controladora, para que libere el actuador correspondiente (selenoide) y se permita el acceso.

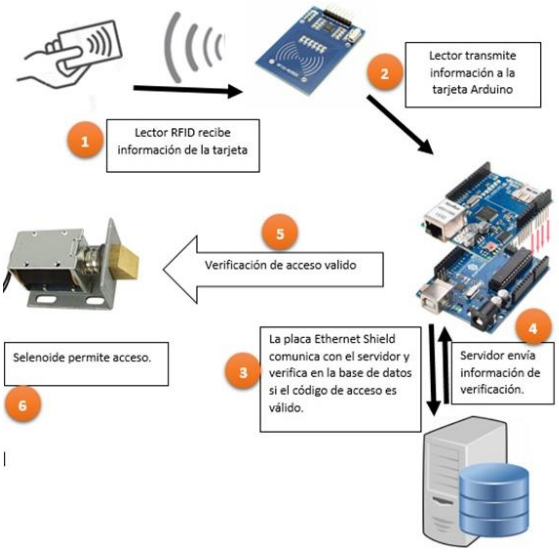

Figura 1 Arquitectura de hardware.

A pesar de ser un diagrama de componentes de hardware, es requisito indispensable establecer una interfaz entre cada uno de los elementos de la figura 1 y que se muestra en la tabla 1. En la tabla 1 se establece la interfaz entre el lector RFID y el componente Arduino, así como también se muestra cómo se conectan cada uno de los pines entre ambos componentes.

Tabla 1 Interfaz de comunicación módulo RFID RC522 y Placa Arduino uno.

Módulo RC522	Arduino UNO
SDA (SS)	10
SCK	13
MOSI	11
MISO	12
IRQ	No conectado
GND	GND
RST	9
3.3 V	3.3 V

Una vez que se realizó la conexión del módulo RC522 con la tarjeta de desarrollo Arduino, se implementó el código para hacer la lectura de las TagID del personal autorizado para acceder al sitio. El código para la lectura de identificación se muestra en la figura 2. La parte importante del código que se muestra en la figura 2, se encuentra en el función loop(), esta es la encargada de llevar a cabo la apertura de la puerta, dado que la función digitalWrite(PUERTIN, HIGH) es quien activa a la contrachapa eléctrica.

```
program showing how to read data from a PICC (that is: a RFID Tag or Card) using a MFRC522
based RFID
Reader on the Arduino SPI interface.
*/

#include <SPI.h>
#include <MFRC522.h>

#define RST_PIN         9          // Configurable
#define SS_PIN          7          // Configurable
#define PUERTIN         6

MFRC522 mfrc522(SS_PIN, RST_PIN);  // Create MFRC522 instance

void setup() {
        Serial.begin(9600);
        while (!Serial);
        SPI.begin();                        // Init SPI bus
        mfrc522.PCD_Init();                 // Init MFRC522
        mfrc522.PCD_DumpVersionToSerial();
        Serial.println(F("Scan PICC to see UID, SAK, type, and data blocks..."));
 pinMode(PUERTIN, OUTPUT);
}

void loop() {
        // Look for new cards
        if ( ! mfrc522.PICC_IsNewCardPresent()) {
                return;
        }

        // Select one of the cards
        if ( ! mfrc522.PICC_ReadCardSerial()) {
                return;
        }

        // Dump debug info about the card; PICC_HaltA() is automatically called
        mfrc522.PICC_DumpToSerial(&(mfrc522.uid));
 digitalWrite(PUERTIN, HIGH);
 delay(9000);
 digitalWrite(PUERTIN, LOW);
```

Figura 2 Código de lectura para la identificación.

Arquitectura de software

Para la implementación de la App móvil, se diseñó una arquitectura de 3 capas y 2 niveles, utilizando el esquema cliente servidor, tabla 2. La capa de presentación, que está alojada en un dispositivo móvil y contiene la interfaz del usuario, junto con la capa lógica que es la encargada de las peticiones y respuestas. Estas dos capas se encuentran en el nivel 1.

Tabla 2 Arquitectura de 3 capas y 2 niveles.

CAPA	NIVEL
Presentación	1
Lógica	2
Datos	

En el nivel 2 se encuentra el servidor y funciona con la capa lógica, ya que es a través de esta capa que se envían las solicitudes de almacenamiento o recuperación de la información a la capa de datos. Este componente se realizó utilizando el lenguaje de programación Java, además de utilizar XML. A continuación, se explican cada una de las capas utilizadas:

- Capa de presentación. Esta capa pertenece a la interfaz gráfica de la App móvil. Para su implementación se usó el IDE Android Studio. En el IDE de Android Studio se requieren dos tipos de archivos para hacer una vista o Activity: XML y Java. El archivo XML contiene los elementos gráficos que son utilizados al generar una Activity (Button, TextView, EditText). Por otro lado, el archivo java contiene el código encargado de asignar acciones a estos elementos gráficos de su correspondiente archivo XML.
- Capa lógica. En esta capa se solicitan los datos por la aplicación a través del método POST, y son enviados a un archivo PHP. En la figura 3 se muestra el código snippet PHP que se encarga de solicitar la información a la base de datos regresando a la aplicación los datos codificados en JSON.
- Capa de datos. En esta capa se encuentra la Base de Datos. En ésta se utilizó como manejador de bases de datos a MySQL. Este manejador es multihilado y multiusuario, además de cumplir con las siguientes funciones:
  - ✓ Manipulación de los datos: responde a las solicitudes del usuario para realizar operaciones de supresión, actualización, extracción, entre otras gestiones. El manejo de los datos ha de realizarse de forma eficiente, según las peticiones realizadas por los usuarios, y permitir la modificación del esquema de la base de datos.
  - ✓ Seguridad e integridad de los datos: Además de registrar el uso de las bases de datos, ante cualquier petición, también aplicará las medidas de seguridad e integridad de los datos previamente definidos.
  - ✓ Recuperación y restauración de los datos ante un posible fallo.

El diseño de la base de datos es sencillo ya que solo consta de una tabla de base de datos, la cual se muestra en la figura 4.

```php
<?php
  $link = mysqli_connect("localhost","guiaturu_dave","W4rM4cH1n52ol7","guiaturu_cti");
  $login = json_decode($_POST["getUsers"]);
  $admin = $login->admin;
        $query = "select * from control";
        $row = mysqli_query($link,$query);
  $existe = mysqli_num_rows($row);
  if($existe>0){
  $response["users"] = array();
        $result = mysqli_query($link,$query);
    while ($row = mysqli_fetch_array($result)) {
      // temp user array
      $users = array();
      $users["name"] = $row["name"];
      $users["phone"] = $row["phone"];
      $users["email"] = $row["email"];
      $users["tagid"] = $row["tagid"];
      array_push($response["users"], $users);
    }
    $response["success"] = 1;
    echo json_encode($response);
  }else{
        $response["success"] = 0;
          // echoing JSON response
        echo json_encode($response);
  }
  mysqli_close($link);
```

Figura 3 Código snippet que procesa la información en PHP.

Figura 4 Diseño de la base de datos para el control de acceso de usuarios.

3. Resultados

El proceso de automatización descrito en este trabajo se implementó en el laboratorio del CTI de la FCC de BUAP y fue realizado por estudiantes de servicio social. Este proceso permite que los estudiantes tengan acceso al mismo utilizando una tarjeta que contiene un TagID. Si no está registrado este elemento, no se permite el acceso. En la figura 5 se muestra la integración de los diferentes componentes de hardware (Módulo RFID RC522, Placa Arduino uno, Placa Ethernet Shield) que permiten automatizar el acceso al laboratorio del CTI de la FCC de la BUAP, aunque es necesario realizar una carcasa que proteja los dispositivos de la intemperie, estos trabajan correctamente.

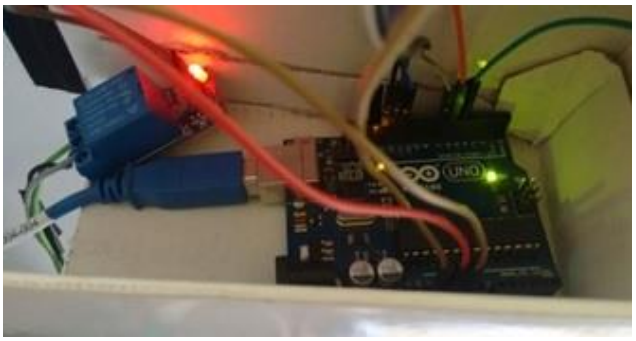

Figura 5 Integración de los componentes de hardware.

La figura 6 muestra las interfaces de la aplicación móvil. En ésta, se muestra la lista de usuarios que tienen acceso al laboratorio, así como la interfaz de acceso del administrador del sistema. Los resultados que se obtuvieron del sistema en su conjunto fueron correctos, éste verifica de forma correcta las tarjetas que tienen acceso al laboratorio y rechaza la entrada a códigos no registrados. La usabilidad de la app es aceptable como se muestra en la figura 6, ya que es eficiente, intuitiva y el tiempo de respuesta es menor a un segundo.

En caso de errores, es necesario verificar que cada componente funcione de forma correcta ya que uno de los inconvenientes que se presentaron fue que la tarjeta lectora RFID tiene fallas, por estar expuesta a la intemperie. Motivo por el cual se tuvo que cambiar de tarjeta, siendo esta reemplazada por una exactamente igual.

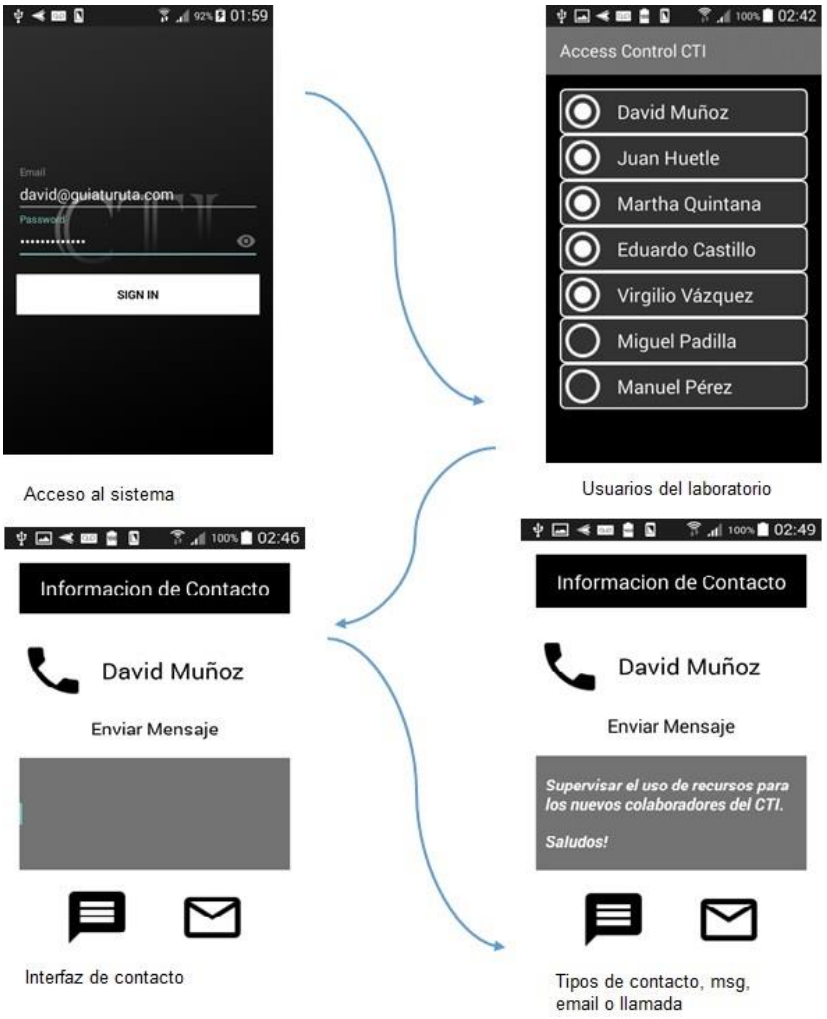

Figura 6 Interfaces de la aplicación móvil.

4. Discusión

RFID es una tecnología que presenta atractivas ventajas contra otras tecnologías de autenticación. El interés por la tecnología RFID se ha incrementado con rapidez. Muchas empresas y gobiernos están buscando aumentar la eficiencia de sus operaciones y reducir costos a través de esta tecnología. El mecanismo de automatización desarrollado abarcó todos los elementos involucrados en uso de la tecnología RFID y dispositivos móviles. Este proyecto se desarrolló con éxito ya que es funcional y permite llevar un control de las personas que acceden a un laboratorio de la FCC de la BUAP. Se utilizaron diferentes tecnologías tanto de software como de hardware y se realizaron las interfaces correspondientes, permitiendo automatizar el mecanismo de acceso al laboratorio. Aunque es un

prototipo ya que no se tiene una carcasa que proteja los dispositivos, el mecanismo de autenticación es funcional y fácil de instalar. Al sensor de RFID también se le puede colocar una carcasa que lo proteja de la intemperie.

La aplicación móvil presenta una interfaz amigable para la configuración de los usuarios del sistema, esto es, agregar, quitar o modificar. La estructura de la base de datos es simple y es modificable para que la aplicación móvil emita alertas de cuando un usuario accede al laboratorio.

Con este proyecto se alcanzó la meta, automatizar el acceso al laboratorio e identificando a los usuarios del mismo. Es importante recalcar que este proyecto es parte de una solución, cuyo objetivo es identificar usuarios utilizando procesamiento digital de imágenes, cámaras, servomotores, dispositivos Raspberry, entre otros.

Por último, el costo total del proyecto se divide en dos partes, software y hardware. Para la segunda, se tiene un gasto aproximado de $1000 pesos, pudiendo ser menor ya que se utilizaron solo dispositivos originales. Respecto al costo de la app, como se explicó anteriormente, se utiliza tecnologías de libre acceso. Si se comercializa este proyecto de manera masiva, se le agregaría al costo del hardware un 50% adicional.

5. Bibliografía y Referencias

[1] Das, S. R., Chita, S., Peterson, N., Shirazi, B. A., & Bhadkamkar, M. (2011, March). Home automation and security for mobile devices. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on (pp. 141-146). IEEE.

[2] Kovatsch, M., Weiss, M., & Guinard, D. (2010, September). Embedding internet technology for home automation. In Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on (pp. 1-8). IEEE.

[3] Rajadurai, S., Nehru, P. P., & Selvarasu, R. (2015, March). Android mobile based home security and device control using GSM. In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on (pp. 1-5). IEEE.

[4] Phillips, T., Karygiannis, T., & Kuhn, R. (2005). Security standards for the RFID market. IEEE Security & Privacy, 3(6), 85-89.

[5] Piyare, R., & Tazil, M. (2011, June). Bluetooth based home automation system using cell phone. In Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on (pp. 192-195). IEEE.

[6] Potts, J., & Sukittanon, S. (2012, March). Exploiting Bluetooth on Android mobile devices for home security application. In Southeastcon, 2012 Proceedings of IEEE (pp. 1-4). IEEE.